

⑪ Int.Cl.

G 06 F 12/14

識別記号

3 2 0

庁内整理番号

B-7737-5B

⑬ 公開 昭和63年(1988)9月20日

審査請求 未請求 発明の数 1 (全3頁)

⑭ 発明の名称 セキュリティ機能付きROM

⑮ 特 願 昭62-59463

⑯ 出 願 昭62(1987)3月13日

⑰ 発 明 者 渡 邊

修

宮城県仙台市一番町2丁目2番13号 富士通東北デジタル・テクノロジー株式会社内

⑱ 出 願 人 富士通株式会社

神奈川県川崎市中原区上小田中1015番地

⑲ 代 理 人 弁理士 井 桁 貞一

明 細 書

1. 発明の名称

セキュリティ機能付きROM

2. 特許請求の範囲

データを記憶するメモリセル部(3)と、
鍵となるパターンを記憶する鍵パターン記憶部(4)
と、
該鍵パターン記憶部の出力と該データを読み出す
際に入力された鍵パターンとを照合して、不一致
なら該メモリセル部に加えるアドレスを覆乱する
アドレス覆乱部(5)とを有することを特徴とするセ
キュリティ機能付きROM。

3. 発明の詳細な説明

〔概要〕

セキュリティ機能付きROMにおいて、ROMの鍵
パターン記憶部に記憶された鍵パターンと新たに
入力した鍵パターンとを照合して、不一致の時に

は入力アドレスを覆乱して誤ったデータを読み出
す様にして、回路規模を大幅に変更することなく
簡単にセキュリティ機能を付加したものである。

〔産業上の利用分野〕

本発明はセキュリティ機能付きROMに関するも
のである。

ROMは多くの電子機器に使用されているが、セ
キュリティ機能が付加されているものは殆どない
ので、これに伴って近年、ROMデータをコピーして
使用するデータ盗用が増加している。

そこで、回路規模を大幅に変更することなく簡
単に、しかも高性能なセキュリティ機能が付加さ
れたROMが必要である。

〔従来の技術〕

第3図は従来例のブロック図を示す。

以下、コントローラ2内のROMには、鍵になる
パターンが書き込まれているとして図の動作を説
明する。

先ず、利用者が外部 ROM 1 からデータを読み出す為に鍵パターンをコントローラ 2 に入力すると、ここに記憶されている鍵パターンと入力された鍵パターンとが比較されるが、不一致の場合には外部 ROM 1 内のメモリセルから読み出したデータを入出力コントローラで覆乱してコントローラ 2 を介して出力したり、又はコントローラから入出力コントローラを制御してデータの読み出しを禁止する。

この為、データの解説が不可能になる。

〔発明が解決しようとする問題点〕

しかし、セキュリティ機能を維持する為に専用コントローラが必要となり回路規模が大きくなるという問題点がある。

〔問題点を解決する為の手段〕

上記の問題点は第 1 図に示すセキュリティ機能付き ROM により解決される。

ここで、3 はデータを記憶するメモリセル部で、

読み出されるので解説は不可能である。

即ち、ROM 内の鍵パターン記憶部 4 で鍵パターンを記憶することにより、専用コントローラが不要となり、回路規模が縮小する。

〔実施例〕

第 2 図は本発明の実施例のブロック図である。

ここで、出力イネーブル/チップイネーブル回路 31、データ入力バッファ 32、アドレスデコーダ 33、出力バッファ 34、メモリセル部 35、データバス 36、アドレスバス 37 はメモリセル部 3 の構成部分、論理回路 51、52、比較論理メモリ 53 はアドレス覆乱部 5 の構成部分を示す。

以下、論理回路 51、52 は EX-OR ゲートで構成するとして図により動作を説明する。

先ず、出力イネーブル/チップイネーブル回路 31 にそれぞれ定められた状態の出力イネーブル OE、チップイネーブル CE、制御信号 CONT (以下、OE、CE、CONT と省略する) と加えて ROM を書き込みモードにする。

4 は鍵となるパターンを記憶する鍵パターン記憶部であり、5 は鍵パターン記憶部の出力と該データを読み出す際に入力された鍵パターンとを照合して、不一致なら該メモリセル部に加えるアドレスを覆乱するアドレス覆乱部である。

〔作用〕

本発明は読み出されたデータを覆乱するのではなく、読み出しアドレス自体を覆乱して誤ったデータを読み出して、データ盗用が行われない様にする。

即ち、予め鍵パターン記憶部 4 に書き込まれた鍵パターンと入力された鍵パターンとをアドレス覆乱部 5 で比較する。

この時、2 つのパターンが一致すれば、データを読み出す為に入力されたアドレスは覆乱されずにメモリセルに加えられて正しいデータが読み出される。

しかし、不一致の場合には上記のアドレスは覆乱され、覆乱されたアドレスに対応したデータが

そして、データをデータバス 36、データ入力バッファ 32 を介してメモリセル部 35 に書き込んだ後、鍵パターンであるランダムパターンをデータバス、データバッファを介して鍵パターン記憶部 41 に書き込む。

しかし、このままでは比較論理メモリ 53 が "オール 0" になっているので、アドレスが入力すれば対応するデータが読み出される。そこで、これを防止する為にデータバス 36、データ入力バッファ 32 を介して EX-OR ゲート 52 に "0" を加えて比較論理メモリ 53 にランダムパターンを書き込む。

次に、出力イネーブル/チップイネーブル回路 31 に別の状態の OE、CE、CONT を加えて ROM を読み出しモードにする。そして、データバス 36、データ入力バッファ 32 を介してランダムパターンを EX-OR ゲート 52 に加える。ここには記憶されたランダムパターンも加えられているので、2 つのパターンが比較され、一致していれば "オール 0" が、不一致なら "オール 0" と異なるパターンが不揮発性メモリで構成された比較論理メモリ 53 に加え

られる。

一方、アドレスバス37、アドレスデコード33を介して入力したアドレスはEX-ORゲート51に加えられるが、一致の時は“オール0”の為にそのままここを通過し、メモリセルから正しいデータが読み出され、出力バッファ34を介して取り出される。

しかし、“オール0”と異なるパターンの時は入力したアドレスは覆乱されて間違ったアドレスとなる。この為、間違ったデータが出力されるので解読が不可能である。

ここで、上記のランダムパターンを多数バイトにわたって設定したり、このパターンを記憶する領域を任意の場所に設定する様にすれば更にセキュリティの強度が増す。

又、論理回路52の位置をメモリセル35の前段に設けたり、出力バッファ34の前段や後段に設けてもよい。更に、この回路52の構成として例えばより複雑な構成にすることも可能である。

即ち、ROM単体でセキュリティ機能を持つので、

ROMごとに異なるランダムパターンを入力すれば個別にセキュリティを行うことができると共に、専用コントローラを使用しないので回路規模が縮小される。

(発明の効果)

以上詳細に説明した様に本発明によれば、回路規模が縮小されると言う効果がある。

4. 図面の簡単な説明

第1図は本発明の原理ブロック図、

第2図は本発明の実施例のブロック図、

第3図は従来例のブロック図を示す。

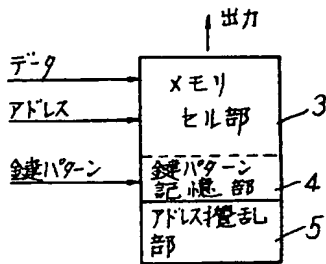
図において、

3はメモリセル部、

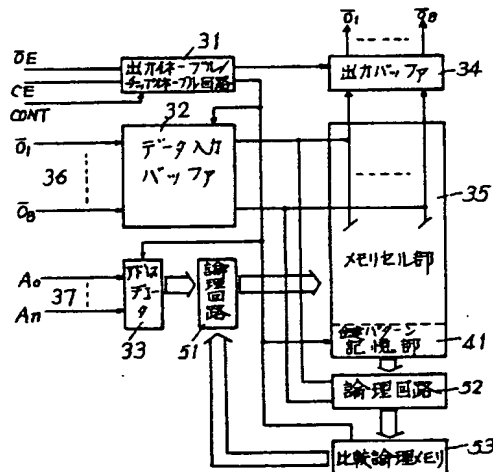
4は鍵パターン記憶部、

5はアドレス覆乱部を示す。

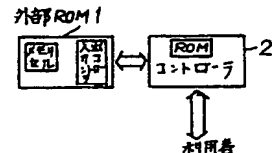
代理人 弁理士 井桁 貞一



本発明の原理ブロック図
第1図



本発明の実施例のブロック図
第2図



従来例のブロック図
第3図